



SECURITY DOMAIN MINUTES

Date: November 21, 2002

Attendees

- | | |
|--|---|
| <input type="checkbox"/> Dustin Bieghler | <input type="checkbox"/> Lora Mellies |
| <input type="checkbox"/> Curt Christian | <input type="checkbox"/> Gail Morris |
| <input type="checkbox"/> Dianna Dees | <input type="checkbox"/> R.D. Porter |
| <input type="checkbox"/> Stephen Derendinger | <input type="checkbox"/> Barry Van Sant |
| <input type="checkbox"/> Barb Kiso | <input type="checkbox"/> Pete Wieberg |
| <input type="checkbox"/> Doug Less | <input type="checkbox"/> Greg Wilson |
| <input type="checkbox"/> Bob Meinhardt | <input type="checkbox"/> |

Agenda Discussion

Detailed notes available



Reviewed November 7th Minutes / New Business

Minutes reviewed and accepted as written.



ITAB Security Minutes Summary:

A portion of the minutes from each of the Security Domain Committee meetings will be summarized and sent to the ITAB Security committee. This will allow that group to have an understanding of what is being covered by the Security Domain Committee.



ITAB NIST Basis Update:

Bob Meinhardt reported that in the ITAB meeting on November 20th Rex talked on the Security Domain committee using the NIST security information as the basis for developing the compliances for the State of MO. There were no objections to that.

Homework protocols:

Dustin Bieghler initiated discussion on protocol for dealing with team deadlines was discussed. At times the Domain Committee has “homework” that is to be turned in on a specific date. When homework does get divided up to the team an individual will be assigned as the contact person to aid in facilitating the consolidation and distribution of the information to the team. If for some reason you cannot make the deadline please let the contact person know so they can distribute what has been collected. Bob Meinhardt wanted to emphasize that the Domain Committee should not be having “homework” every time it should be rare that it does happen.

ITAB Meeting Invitation:

Bob Meinhardt and Doug Less wanted to invite the Security Domain Committee to come to the ITAB meeting on January 29, 2003. This ITAB meeting will include a 2.5-hour presentation on Architecture. Including some of the work the Security Domain Committee has done to-date as well as how to move the other Domain Committees forward and man them.

January Security Domain Potential meeting dates:

A review of potential Security Domain Committee meeting dates was discussed. All agreed that no meeting would be held on January 2, 2003. Proposed dates include:

- ☐ January 9, 2003
- ☐ January 16, 2003
- ☐ January 30, 2003

January 23, 2003 is not included due to the fact that it will most likely be the ITAB Security Committee meeting date. These dates will be confirmed with the group and a schedule will be sent out.

NIST Subject Area Homework Review

NIST Subject Areas Covered:

- ☐ Data Integrity Controls – Pete Wieberg
- ☐ Logical Access Controls – Dustin Bieghler
- ☐ Hardware & Systems Software – Curt Christian
- ☐ Incident Response Capability – R.D. Porter
- ☐ Personnel Security – Lora Mellies
- ☐ Physical Security – Steve Derendinger
- ☐ Security Awareness, Training and Education – Gail Morris

The worksheets were reviewed. The definitions of the 3 disciplines were identified from NIST information. Then the various Technology Areas were then determined based on the reviewed information. The Technology Areas were then mapped to the 3 disciplines that had been identified. This information is covered below.



Structure of the MAEA Blueprint



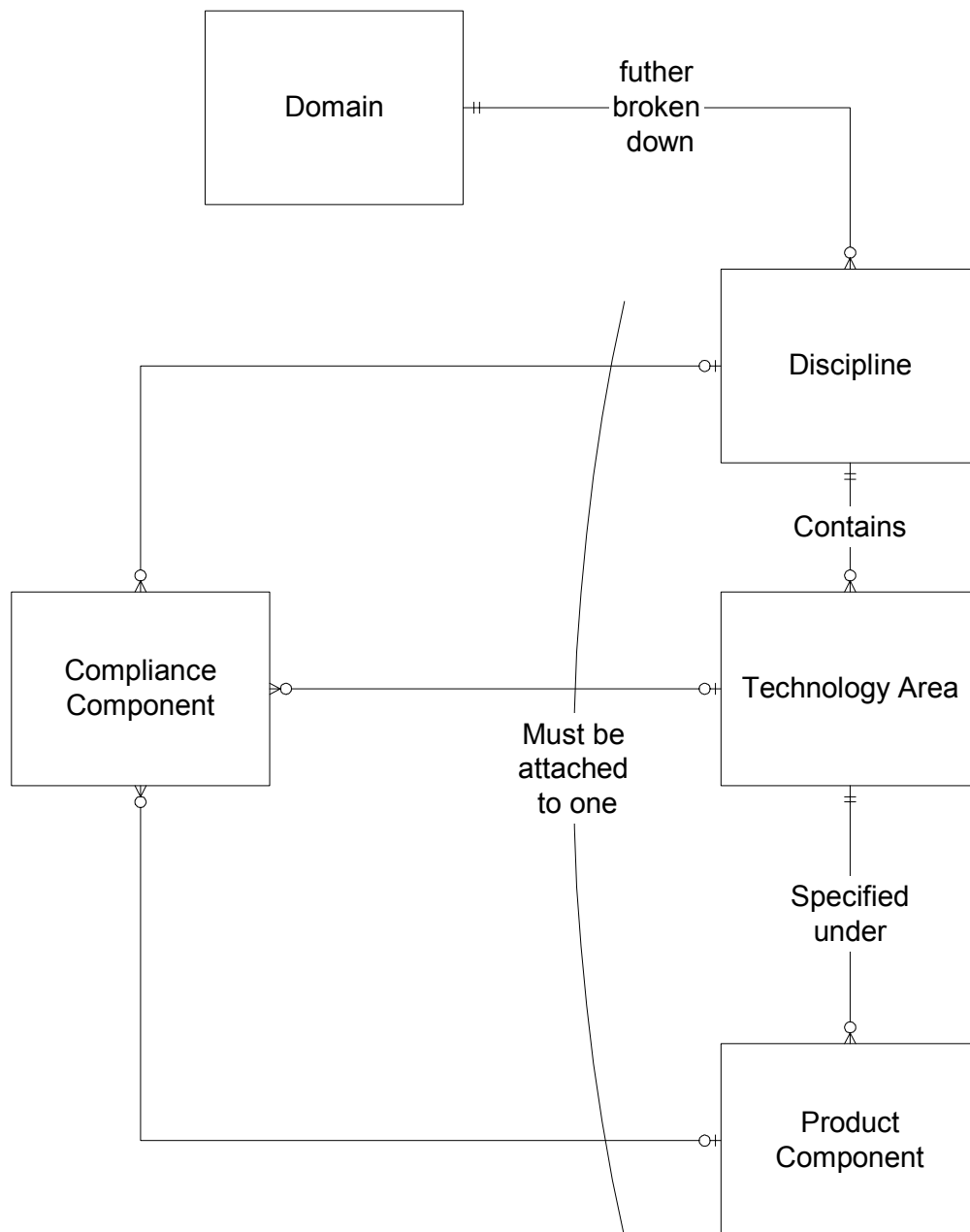
There was some confusion between Subject Areas and Technology Areas in the MAEA blueprint. The following are the definition that are covered in the MAEA Manual Part III Appendix B:

- ❑ Subject Areas are topics within a Discipline that help to define the boundary of the Discipline and its parent Domain. Subject Areas are an additional layer of detail that provides the Domain committees with general descriptions of technology topics relevant to each Discipline.
As an example, in the MAEA Infrastructure Domain, the Platform Discipline can be further defined to include the following Subject Areas:
 - Hardware
 - Operating Systems
 - Utilities
 - Provisioning
- ❑ Technology Areas are those technical items or topics that support the functionality of the architecture. Technology Areas are associated to a given Discipline (a Discipline is composed of multiple technology areas). Product and Compliance Components are associated with a Technology Area.

To further clarify this the group talked about the fact that subject areas are provided to help define the scope of a discipline and/or domain. This has been added as one of the items to address in the MAEA version 1.2 updated. So as not to cause more confusion Subject Areas will be renamed to be more consistent with their intended use in defining scope and boundary.

■ MAEA Blueprint Entity Relationship Diagram

Dianna drew the following relationships to help further define the relationships between the 5 templates in the MAEA Blueprint. Subject Areas are an attribute on both the domain and discipline templates to help clarify the boundary.



Security Domain Initial Discipline Definitions

Management Controls

Management Controls addresses security topics that can be characterized as managerial. They are techniques and concerns that are normally addressed by management in the organizations computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization.

Operational Controls

Operational Controls addresses security controls that focus on controls that are, broadly speaking implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems.) They often require technical or specialized expertise – and often rely upon management activities as well as technical controls.



Technical Controls

Technical Controls focuses on security controls that the computer system executes. These controls are dependent upon the proper functioning of the system for their effectiveness. The implementation of technical controls however, always requires significant operational considerations – and should be consistent with the management of security within the organization.








Security Domain Technology Areas

Management Controls	Operational Controls	Technical Controls
Information Classification	Authorization	Access Controls
Personnel Security	Data Verification	Cryptography
Security Risk Management	Event Monitoring / Analysis	Date / Time Controls
Vulnerability Assessment	Fire/Safety Factors / supporting Utilities	Entity Authentication
	Incident Response	Intrusion Detection System (IDS)
	Message Authentication	Inactivity Controls
	Password Policy Controls	Log-on Banner
	Penetration Testing	Remote Access
	Physical Access Control	Secure Gateways / Firewalls
	Portable System Controls (Part of Physical Access Control)	
	Security Awareness / Education	
	Security Skills Training / Certification	
	Virus Detection & Elimination	

Technology Area Conversation

-  Port Protection - This topic will be addressed as a compliance component under O/S configuration.
-  Event Monitoring may need to be flushed out to have a complete Security Blueprint.

Technology Area Priorities

-  Priority #1 - Incident Response: Based on information for compliance being documented in the ITAB Incident Reporting Procedure and the INFOCON (The Information Operations Condition) this Technology Area will be completed first.
-  Priorities #2 – Two Technology Areas were discussed to be after the Incident Response.
 -  Virus Detection & Elimination
 -  Password Policy Controls
-  Priorities #3 – Two Technology Areas were discussed to be after the Priority #2 Areas:
 -  Information Classification
 -  Secure Gateways / Firewalls

Action Items



Committee:

- ❑ Put ITAB meeting of January 29, 2003 on your calendars. **January 29, 2003**



Architecture Office:

- ❑ Determine process to pass information between Domain Committees. Security Domain has determined 3 areas that need to be populated to have a comprehensive security blueprint:
 - Business Continuity - Assure backup for recovering possible missing data.
 - Infrastructure Domain – For Operating Systems assure port Protection is addressed.

December 19, 2002



D. Cape / Doug Less:

- ❑ Create draft of Incident Response Technology Area and Compliance Component architecture blueprint information. **December 5, 2002**
- ❑ Create draft of Security Domain Discipline templates for Management Controls, Operational Controls, and Technical Controls. **December 5, 2002**